Vzorčni primeri omrežnih incidentov

Gorazd Božič
SI-CERT, ARNES, Jamova 39, Ljubljana
gorazd.bozic@arnes.si

Sirikt 2007, Kranjska Gora, 19. 4. 2007

SI-CERT

Akademska in raziskovalna mreža Slovenije

- pričetek leta 1995
- obravnava varnostnih incidentov na omrežju
- strokovno svetovanje
- obveščanje javnosti
- (forenzika)

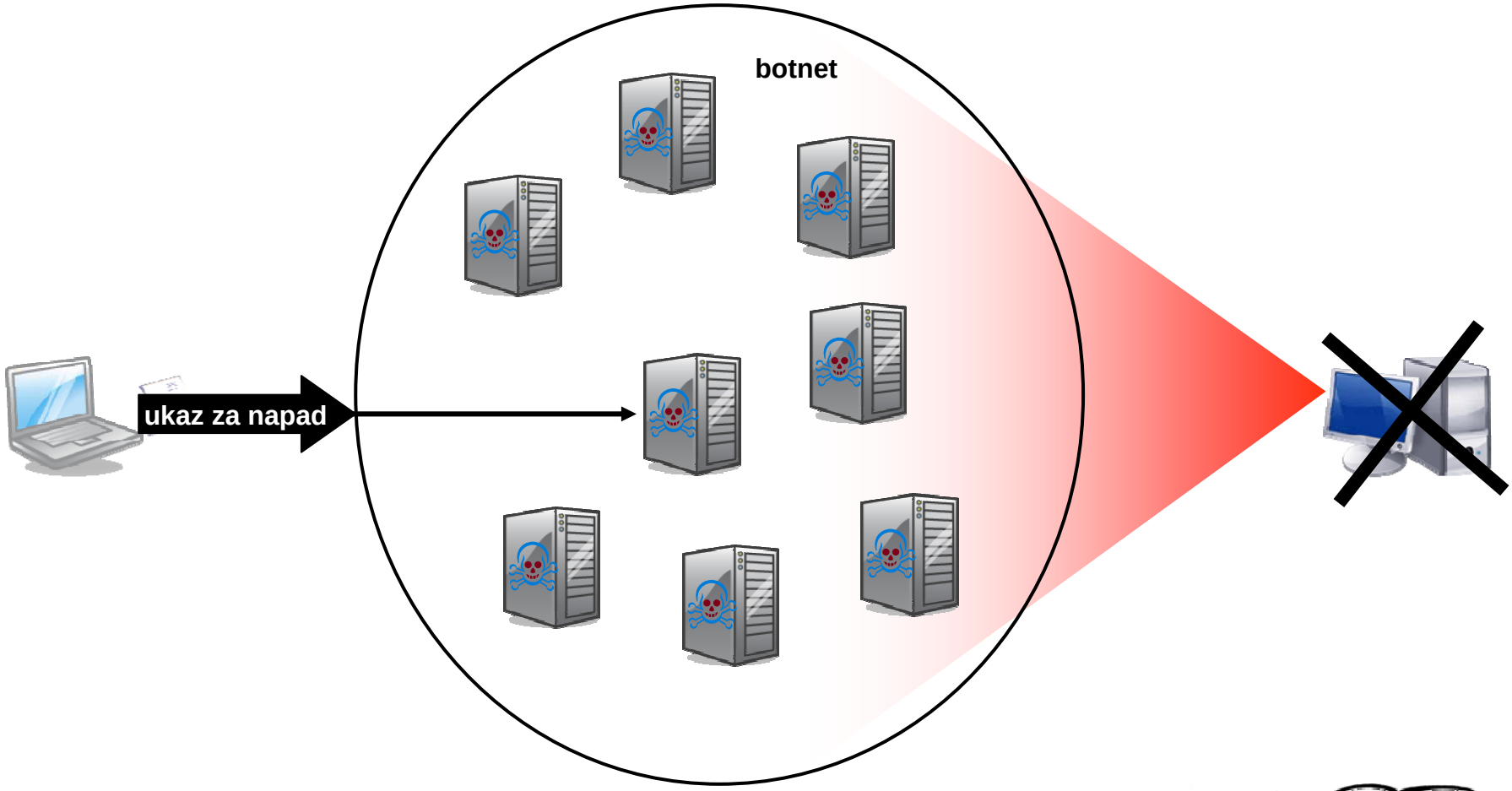
Primer 1: “Virus za učitelco”

Akademska in raziskovalna mreža Slovenije

```
[ 14:02:16 ] [ @Bl4cky ] PLISS KDO VE: jaz bi rabo nek virus :D za učitelco da bi ji poslal neki
                         po mailu pa bi ona to odprla in bi se ji naloil virus in bi jaz lahko
                         pol dostopil do njenih podatkov ? :DDD
[ 14:02:17 ] [ @SeNcA ] JUMP DA FUCK UP
[ 14:02:17 ] [ @Bl4cky ] :DDDDDD
[ 14:02:20 ] [ @Bl4cky ] rabim test
[ 14:02:23 ] [ @Bl4cky ] in ga ima na pcju
[ 14:02:26 ] [ @SeNcA ] bl4cky
[ 14:02:29 ] [ @SeNcA ] ownaj boxo
[ 14:02:29 ] [ @SeNcA ] :D
[ 14:02:33 ] [ @Bl4cky ] lol
[ 14:02:34 ] [ @Bl4cky ] če ima
[ 14:02:35 ] [ @Bl4cky ] arne
[ 14:02:36 ] [ @Bl4cky ] s:
[ 14:02:36 ] [ @SeNcA ] ja
[ 14:02:37 ] [ @SeNcA ] :D
[ 14:02:37 ] [ @Bl4cky ] :D
[ 14:02:39 ] [ @SeNcA ] lol
[ 14:02:40 ] [ @Bl4cky ] pa sploh ne irca
[ 14:02:41 ] [ @SeNcA ] lamerks
[ 14:02:42 ] [ @SeNcA ] lamerka*
[ 14:02:43 ] [ @Bl4cky ] preko maila
```

Botnet in DDoS napadi ("dosanje")

Akademska in raziskovalna mreža Slovenije



Primer 2: "Cyber-bully"


```
[TeŽaK]: maš jurja štirosto
[TeŽaK]: ?
------------: 1000 mam
[TeŽaK]: juter
[TeŽaK]: v sql da daš
[TeŽaK]: 400 pa ko boš mel
[TeŽaK]: ok?
```

Prijatelj Martin

[18:04:42] Martin: kwa je zdaj ti n00b?
[18:04:46] -------: kaj
[18:04:49] Martin: a bo keš?
[18:04:52] Martin: pička ti čorava
…
[18:06:13] -------: sam v čem je finta da nas dosaš
[18:06:16] Martin: k bom kr dosnu
[18:06:26] Martin: kwa v čem?
[18:06:29] Martin: ker niste keš poslali
…
[18:06:50] -------: če pa naprej smo lahk igrali
[18:06:55] -------: pol pa kr da mormo plačat
[18:06:58] -------: neja mormo kr tak hitro
[18:07:30] -------: ja komu te naj dam dnar
[18:07:40] Martin: ma tale tžak te sploh ni ddoso kak 1 tedn ko sploh
…
[18:10:26] Martin: v pondelek da daš tžaku
[18:10:37] Martin: oz. bom kr dau dosat
…
[18:11:19] Martin: k ste v januarju sam vi igrlai
[18:11:22] Martin: mi nč
[18:11:23] Martin: tk da
[18:11:31] -------: ja zakaj niste prej rekli

TeŽaK je podjeten

Akademska in raziskovalna mreža Slovenije

Subject:
From: [redacted]@hotmail.com>
Sender: si-cert-bounces@arnes.si
Reply-To: si-cert@arnes.si
Date: 22.2.2006 19:05
To: si-cert@arnes.si

Pozdravljeni!

Imam ponudbo. Zasačo sem več ddosnetov in ker vem da to ni prav sem se odločil da bom prijavo na arnes. Sem tip, ki sem zelo proti 'heckanju' in 'ddosanju' in zato takšne ljudi tudi prijavljam. Vedaj pa me nekaj zanima. Kakšno nagrado bi lahko dobil, če bi vam izdal par serverjov in ljudi za katere sem 100% da imajo te zadeve, ker bi te ljudi zlahka najdli tudi če bi jih nadzorovali do 5dni!
Nagrade bi lahko bile takšne:
2mb paket za 1 leto ali denarna valuta.
Upam da se boste pogovorili z šefom arnesa in sklenli kako boste. Če se boste strinjali vam lahko jaz prvi izdam podatke o teh ljudeh in nato daste nagrado.
LP

Express yourself instantly with MSN Messenger! Download today it's FREE!
http://messenger.msn.click-url.com/go/onm00200471ave/direct/01/

SIRIKT 2007

Phishing


http://212[redacted]aypal/
Google
PayPal
Sign Up | Log In | Help
Welcome
Send Money
Request Money
Merchant Services
Auction Tools
Member Log-In
Forgot your email address?
Forgot your password?
Email Address
Password
Log In
Join PayPal Today
Now Over
100 million accounts
Sign Up Now!
Learn more about
PayPal Worldwide
Shop Without Sharing
Your Financial Information
PayPal. Privacy is built in.
Learn more
PayPal Mobile
Learn more
Buyers
Send money to anyone with an email address in 55 countries and regions.
PayPal is free for buyers.
Shop without sharing financial information.
100% protection against unauthorized payments sent from your account.
eBay Sellers
Free eBay tools make selling easier.
PayPal works hard to help protect sellers.
PayPal simplifies shipping and tracking.
Earn cash back with PayPal Preferred Rewards.
Merchants
Accept credit cards online with PayPal.
Get paid by phone, fax, and mail with Virtual Terminal.
See how PayPal can increase your sales.
Learn more about our secure Merchant Services.
Compare our solutions side by side
About | Accounts | Fees | Privacy | Security Center | Contact Us | User Agreement | Developers | Jobs | Mobile | Blue Card | Referrals | Shops | Mass Pay

Phishing - tudi pri nas

Akademska in raziskovalna mreža Slovenije

Opozorilo! Pojav ponarejene vstopne strani za SiOL-ovo s

Uporabnike SiOL-ove spletne pošte, ki do elektronske pošte dostopate preko SiOL opozarjamo, da se je na spletu pojavila škodljiva programska oprema, ki simulira vs pošte (do katere dostopate preko posta.siol.net/). Lažni spletni strani od uporabr uporabniškega imena in gesla, nahajata pa se na spletnih naslovih www.siol.co.n

Opozarjamo vas, da uporabniškega imena in gesla v nobenem primeru ne vnašate. če sumite, da je prišlo do zlorabe, nemudoma pokličite SiOL-ov Center za pomoč u številko 080 1000 ali pošljite elektronsko sporočilo na info@siol.net

Namen tovrstnih spletnih strani je kraja zaupnih podatkov uporabnikov – v tem primeru gesel, bo »phishing«. Napadalci ciljajo predvsem na nepozorne uporabnike, ki zaradi pristnega videza e-s hudega sluteč vnesejo svoje geslo.

Da boste znali razločiti med pravo in ponarejeno vstopno stranjo za SiOL-ovo spletno pošto, sm prikaz razlik.

Klik NLB | Osebne finance | Poslovne finance

Poti do banke | Klik NLB

Klik NLB

Pozor! Pojav ponarejene vstopne strani NLB Klika

Uporabnike NLB Klika stalno opozarjamo na pojavljanje škodljive programske opreme, ki se na različne načine (npr. ob obisku spletnih strani, prek e-pošte, z nameščanjem opreme "sumljivega" izvora) namesti na osebni računalnik uporabnika. Zlikovcem omogoča prevzem nadzora nad vašim računalnikom na daljavo in beleženje vseh vnešenih podatkov. Tako so odprta vrata za krajo, saj lahko s tako pridobljeni osebnimi in elektronskimi identifikacijskimi podatki, zlikovci dostopajo do vseh storitev v vašem imenu.

Vse več pojavov "ribarjenja" oz. Phishing podatkov

V zadnjem času je v svetovnem merilu vse bolj aktualen trend povečevanja števila elektronskih sporočil ali spletnih strani, ki navidezno izgledajo kot prava stran ponudnika spletnih storitev. Od uporabnika zahtevajo vnos določenih podatkov - **predvsem varnostnih elementov**, ki jih sicer originalni ponudniki spletnih storitev ne zahtevajo. Gre za zlonamerno pridobivanje podatkov, znano kot "ribarjenje" oz. "phishing". Pogoj za uspešen "ulov podakov" je, da nepozoren uporabnik vnese zahtevane podatke oz. izvede zahtevane aktivnosti. Tak način zlonamernega zbiranja podatkov je v svetu znan že nekaj časa in zlikovcem omogoča, da vaše varnostne elemente v vašem imenu zlorabijo v svojo korist.

Uporabnike NLB Klika posebej opozarjamo, da smo v teh dneh ugotovili pojav nove škodljive programske opreme, ki simulira lažni vstopni ekran NLB Klika. Od uporabnika zahteva izvoz kvalificiranega digitalnega potrdila ter vnos različnih gesel.
Da boste znali razločiti med pravo in ponarejeno vstopno stranjo v NLB Klik, smo za vas pripravili kratke opise in prikaze razlik ter varnostnih opozoril, če tako stran zaznate.

Opis in prikaz razlik med pravo in ponarejeno vstopno stranjo v NLB Klik

Primer 3: "Carding"

Akademska in raziskovalna mreža Slovenije

- sumljiv promet iz knjižnice
  - skeniranje vrat 22, Secure Shell
- na računalniku je IRC strežnik
  - predstavlja se kot irc.tunisia.org
- na njem je kanal #CcPoWeR

```
There are 250 users and 86 invisible on 8 servers
32 :operator(s) online
49 :channels formed
I have 3 clients and 1 servers
Current Local Users: 3  Max: 72
Current Global Users: 336  Max: 357
-  Message of the Day -
- 13/1/2007 22:07
-                                                $,  $,     ,
-                                              "ss.$ss. .s'
-                                     ,     .ss$$$$$$$$$$s,
-                                    $. s$$$$$$$$$$$$$$`$$Ss
-                                    "$$$$$$$$$$$$$$$$$$o$$$       ,
-                                   s$$$$$$$$$$$$$$$$$$$$$$$$s,  ,s
-                                  s$$$$$$$$$"$$$$$$"""$$$$$$"$$$$$,
-                                  s$$$$$$$$$s""$$$$ssssss"$$$$$$$"
-                                 s$$$$$$$$$$'         `"""ss"$"$s""
-                                 s$$$$$$$$$$,              `"""""$  .s$$s
-                                 s$$$$$$$$$$$$s,...               `s$$'  `
-                             `ssss$$$$$$$$$$$$$$$$$$$$####s.     .$$"$.   , s
-                              `""""$$$$$$$$$$$$$$$$$$$$$$$$##########$"     $.$'
-                                    "$$$$$$$$$$$$$$$$$$$$$$$$s""     .$$$|
-                                     "$$$$$$$$$$$$$$$$$$$$$$$$s    .$$" $
-                                      $$""$$$$$$$$$$$$$$$$$$$$$$$$$$"   `
-                                      $$"  "$"$$$$$$$$$$$$$$$$$S""""'
-                                     ,  ,"     '  $$$$$$$$$$$$$$$$$$s
-                                     $.          .s$$$$$$$$$$$$$$$$$$"
-                    ,                "$s.   ..ssS$$$$$$$$$$$$$$$$$$"
-                   $                 .s$$$S$$$$$$$$$$$$$$$$$$$$$"
-                   Ss     ..sS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$""
-                    "$$$sS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$"
-                ,     s$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$""'
-               $    s$$$$$$$$$$$$$$$$$$$$$$$$$$$$""'      s'       ,
-              $$..$$$$$$$$$$$$$$$$$$$$$$$$$$$$"'       ....,$$....    ,$
-               "$$$$$$$$$$$$$$$$$$$$$$$$$$$"' ,     .sS$$$$$$$$$$$$$$$s$$
-                 $$$$$$$$$$$$$$$$$$$$$$$$$"     $, .s$$$$$$$$$$$$$$$$$$$.
-     )           $$$$$$$$$$$$$$$$$$$$$$$$'      `$$$$$$$$$$$$$$$$$$$$$$$$$.
-    ((           $$$$$$$$$$$$$$$$$$$$$$$       $$$$$$$$$###       "$$$$$$$$$$$$$
-     ) \         $$$$$$$$$$$$$$$$$$$$$.     $$$$$$$$$"             "$$$$$$$$$$   s'
-    (   )        $$$$$$$$$$$$$$$$$$$$.   $$$$$$$$"                 $$$$$$$$$$$$s$'
-    )  ( (       $$"$$$$$$$$$$$$$$$$$.$$$$$$$$'   .$$$$$$$$$$$$"
-    (  )  )   _,$"   $$$$$$$$$$$$$$$$$$.$$$$'     DoS         .$$$$$$$$$$$$$
-    ) (  ( \.         "$$$$$$$$$$$$$$$$$$,,,.           ..$$$$$$$$$$$$$$"
-   (   )$ )  )        ,$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$"
-   (   ($$  ( \     _sS"  `"$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$S$$,
-    ) )$$$s ) )  .       .   `$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$"'  `$$
-     (   $$$Ss/  .$,    .$,,s$$$$$$$$S$$$$$$$$$$$$$$$$$$$$$$$$S""        '
-      \)_$$$$$$$$$$$$$$$$$$$$$$$$$$$"  $$         `$$.         `$$.
-          `"S$$$$$$$$$$$$$$$$$$"      $           `$           `$
-              `""""""""""""""'         '           '            '
          (3)  5
`-irc.audnet.net          (24)  200
  |-irc.co.in             (5)  125
  |-k9.audnet.net         (1)  185
  |-matrix.audnet.net     (7)  150
  `-irc.p00n.org          (46)  155
```

Kaj se prodaja?

Akademska in raziskovalna mreža Slovenije

```
                  07-02-04 10:38:21 Speed-        Card Holder Name: Richard E [redacted]
                  07-02-04 10:38:22 Speed-        Address 1 : 4415 [redacted] Ave
                  07-02-04 10:38:22 Speed-        Address 2 :
                  07-02-04 10:38:22 Speed-        City : Orlando
                  07-02-04 10:38:22 Speed-        State : FL
                  07-02-04 10:38:22 Speed-        Zip Code : 32808
                  07-02-04 10:38:22 Speed-        Phone Number : 4072[redacted]
                  07-02-04 10:38:22 Speed-        Driver's License : S5207[redacted]
                  07-02-04 10:38:22 Speed-        Creditcard Number: 4744[redacted]
07-02-03 21:10:00 ^07-02-04 10:38:22 Speed-                                          ith DOB+SSN,
                  07-02-04 10:38:22 Speed-        Exp Month : 11                      accounts 2$ each,
                  07-02-04 10:38:22 Speed-        Exp Year : 2010                    chovia, halifax,
                  07-02-04 10:38:23 Speed-        Cvv : [redacted]                   or country) 3$,
                  ...
                  07-02-05 15:15:42 san    Email: [redacted]@tinyonline.co.uk
07-02-03 21:12:01 ^07-02-05 15:15:44 san    Password: giles                          + HaCked Hosts +
                  07-02-05 15:15:44 san    CCtype: MASTERCARD                      aCked Shells/Roots,
                  07-02-05 15:15:44 san    CCName: Giles [redacted]
                  07-02-05 15:15:44 san    CCNum: 5505[redacted]
                  07-02-05 15:15:44 san    CVV2: [redacted]
                  07-02-05 15:15:44 san    CCstartdate: 02/05
                  07-02-05 15:15:44 san    CCexp: 02/07
                  07-02-05 15:15:44 san    Address: 5 [redacted]
                  07-02-05 15:15:44 san    City: Lewes
                  07-02-05 15:15:44 san    Postcode: BN8 4EZ
                  07-02-05 15:15:44 san    Phone: 01825 [redacted]
                  07-02-05 15:15:45 san    Country: UK
```

Zaključne misli

- čas nedolžnosti je mimo
- hitro in ustrezno odzivanje
- širjenje nadzora
- prednosti > slabosti
- “zdrava pamet”, previdnost, ozaveščanje